REMARKS

By this Amendment, claims 1 and 6 are amended. Reconsideration and prompt allowance of claims 1-3 and 5-8 is respectfully requested.

Claims 1-3 and 5-8 under 35 U.S.C. §103(a) over U.S. Patent No. 6,076,168 to Fiveash et al. in view of one or more of U.S. Patent No. 5,937,159 to Meyers et al.; U.S. Patent No. 5,983,350 to Minear et al., non-patent document S. Kent, BBN corp.; "Security Architecture for the Internet Protocol, Request for Comments: 2401," November 1998 ("RFC 2401"); and non-patent document S. Kent, BBN corp., "IP Encapsulating Security payload (ESP), Request for Comments: 2406," November 1998 ("RFC 2406"). Based upon the amendments to claims 1 and 6, these rejections are respectfully traversed.

In the Office Action of October 3, 2007, the Examiner asserts that claims 1 and 6 are unclear as to what features are based upon the MAC security class.

Independent claims 1 and 6 are amended to more clearly recite, *inter alia*, wherein the trusted header is applied without user manipulation if a destination node is a secure OS to which the MAC is applied, and the user has a security class. Applicants respectfully submit that the applied art fails to disclose, teach, or suggest at least this feature.

More specifically, Applicants disclose a system wherein if a destination node is a secure OS to which the MAC is applied and the user has a security class, a trusted channel is applied. At this time, if data to be transmitted includes the MAC information, the data and the MAC information is transmitted together. Because the MAC information remains at the destination node, the data is thereby protected. At least this feature distinguishes Applicants' system from that of the applied references.

For example, unlike the Applicants' method and apparatus, packet protection offered by the IPSec protocol, as disclosed in RFC2401 and RFC2406, is based on a security policy database that is set and maintained by a user, a system manager, or an application. More specifically, an encryption section of the packet is set based on the user's need and the packet is encrypted and transmitted. However, Applicants respectfully submit that IPSec does not have a function for transmitting access control information of a user who remotely accesses an OS to which a control

access policy, such as MAC, is applied. In IPSec, if data to be transmitted includes the MAC information, the MAC information is reset after the data is transmitted to the destination address.

Applicants respectfully submit that none of the applied art discloses, teaches or suggests at least this feature, as recited in amended independent claims 1 and 6. Applicants respectfully submit, therefore, that independent claims 1 and 6 are patentable over the applied art, either alone or in permissible combinations. Claims 2-3, 5, and 7-8 are likewise patentable over the applied art at least based on their dependency on an allowable base claim, as well as for additional features they recite. Withdrawal of the rejection over the applied art is respectfully requested.

In view of the foregoing, Applicants respectfully submit that the application is in condition for allowance and favorable reconsideration and prompt allowance of claims 1-3 and 5-8 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,
LOWE HAUPTMAN HAM & BERNER, LLP

/Yoon S Ham/
Yoon S. Ham
Registration No. 45,307

Customer Number: 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: February 4, 2008